IN THE UNITED STATES ARMY
FIRST JUDICIAL CIRCUIT

U N I T E D S T A T E S	)	
	)	**DEFENSE RENEWAL OF**
v.	)	**MOTION TO COMPEL**
	)	**DISCOVERY OF COMPUTERS**
MANNING, Bradley E., PFC	)	
U.S. Army, (b) (6)	)	
Headquarters and Headquarters Company, U.S.	)	
Army Garrison, Joint Base Myer-Henderson Hall,	)	DATED: 30 March 2012
Fort Myer, VA 22211	)	

RELIEF SOUGHT

1. PFC Bradley E. Manning, by counsel, pursuant to R.C.M. 701(a)(6) and 701(2)(A) and applicable case law, requests this Court to order the Government to conduct searches on the relevant computers as outlined in this motion. If the Court does not grant this Order, the Defense requests specific findings of fact and law on the record.

FACTS

2. On 23 March 2012, the Court granted the Defense Motion to Compel Discovery in part with regard to the 14 hard drives from the Tactical Sensitive Compartmented Information Facility (T-SCIF) and the Tactical Operations Center (TOC) of Headquarters and Headquarters Company (HHC), 2nd Brigade Combat Team (BCT), 10th Mountain Division, Forward Operating Base (FOB) Hammer, Iraq. The Court Ordered the Government to immediately cause an inspection of the 14 hard drives for the presence of "Wget, M-IRC Chat, Google Earth, movies, games, music and any other specifically requested program from the Defense." *See* Ruling: Defense Motion to Compel Discovery, p. 11.

3. The Defense, in consultation with its computer forensic experts, proposed a process that would accurately identify any unauthorized music, movies, games, or other programs. The process could be easily completed within a matter of a few days and would not reveal the content of any file. Thus, the information revealed would not be classified, and would not necessitate a review by any Original Classification Authority (OCA).

4. The process recommended by the Defense involved the Government's forensic experts providing the Defense with an EnCase Folder Structure in .rtf format that includes the filenames within each of the following folders for every identified user profile on each hard drive:

a. Program Files;

b. User Profile Storage regarding: Music, Games, Pictures, Local Settings\Application Data; (the Defense has eliminated any reference to "documents" and "etc." in order to avoid any confusion by the Government);

c. Windows\Prefetch; and

d. The following four paths[1]: (1) Documents and Settings\<username>\Local Settings\Application Data\; (2) Documents and Settings\<username>\Application Data\; (3) Users\<username> \AppData\Local; and (4) Users\<username>\AppData\Roaming.

5. The Government opposed the Defense request stating that the list of file names would likely also list classified information because many filenames have actual classified information in the names, such as the ones the accused has been charged with compromising. [Email from MAJ Ashden Fein, March 26]. The Government also stated that its position is that the Defense should be able to at least articulate what unauthorized software it believes is on the hard drives, "otherwise this is a classic fishing expedition for classified information." *Id.* With a Defense provided list, the Government stated that its expert could search the drives and determine whether the information is actually on the drive.

6. The Court tentatively ruled that it would not force the Government to identify all programs on the 14 hard drives. The Court's position was based, in part, upon a belief that the Government did not concur with the Defense that the process could easily be accomplished without the need for a lengthy delay.

7. Based upon the concerns of the Court, the Defense contacted its computer forensic experts again and asked if there were an easier process that would eliminate the Government's objections and the Court's concerns. Mr. Trent Struttmann, one of the Defense computer forensic experts, suggested an even simpler process. This process will allow the Government to obtain only a list of installed programs. According to Mr. Struttmann, the process can be achieved in <u>less than five minutes.</u> The proposed process is as follows:

a. Load up the case file;

b. Run the "Case Processor" and select "Windows Initialize Case";

c. Choose to run the "software" module;

d. Hit "OK" and then wait for the process to finish.

8. Mr. Struttmann maintains that the Case Processor should take less than 30 seconds to complete its task. Once the task is completed, the user simply needs to go to the bookmarks tab. Within the bookmarks tab, one will see a "Software Info" folder that the Case Processor has just created. The user then needs to hit the "Report Tab" and export the results to a RTF list. This

[1] Each identified path was not specifically detailed in the Defense's original request, but is now being identified in order to be responsive to the Government's concern of revealing classified information. The listed paths will avoid any classified documents or classified content.

would then complete the entire process. Once complete, one would have a complete and accurate list of all software (and only the software) on the computer by name without any other information. This process would only provide a list of software. The Government would then need to separately identify any unauthorized music or movies.

WITNESSES/EVIDENCE

9. If the Government does not stipulate that the above process is accurate, the Defense requests the testimony of Mr. Trent Struttmann for the purposes of this motion.

ARGUMENT

10. The Defense believes it is entitled to discovery of the relevant computers under R.C.M. 701(2)(A) as being "tangible objects … which are within the possession, custody or control of military authorities, and which are material to the preparation of the defense." The Defense also maintains that if the computers contain the software that the Defense has reason to believe they contain, then this information would be classic *Brady* material that the Government is obligated to disclose to the Defense under R.C.M. 701(a)(6).

11. While the Defense believes that it is entitled to inspect the actual computers (or a digital image thereof), in the interest of expediency, the Defense is amenable to having the Government perform a meaningful search of the computers for the requested information. As submitted to the Court, the Defense proposes that the Government's forensic experts follow a simple process that will yield a list of program/software names. This, in turn, can be compared against the list of 94 authorized programs to determine how pervasive the practice of adding of "unauthorized" software was in the T-SCIF and TOC.

12. The Defense's tentative theory is that all or most soldiers in the SCIF had unauthorized software on their computers (e.g., M-IRC Chat, Google Earth, Wget, movies, music, games, etc.). This is amply supported by the Article 32 testimony. The Defense intends to show that the practice of adding "unauthorized" software was so pervasive that, in effect, all "unauthorized" programs were implicitly or explicitly authorized. As aptly stated in this Court's ruling, the Defense's theory is that "the information is relevant to establish the defense theory that the addition of software not on the approve list of authorized software was authorized by the accused's chain of command through the practice of condoning and implicitly or explicitly approving the additions of such software." (Ruling: Defense Motion to Compel Discovery, p. 4). Simply because the Government does not believe this is a viable defense does not mean that the Defense should not be able to pursue it and advance it at trial, if there is evidence to support it.[2]

[2] The Court alludes to the fact that the "Defense has evidence from the Article 32 witnesses to further the Defense's theory" – thus suggesting that a full search of the computers is not necessary. While the evidence at the Article 32 hearing certainly supports the Defense's theory, it does not establish just how widespread the practice was.

13. The Defense also believes that if the search yields the expected results (i.e. that it was common for soldiers to add unauthorized software), this is classic *Brady* material under R.C.M. 701(a)(6). The Defense would argue that this would reasonably tend to negate or reduce guilt for the charged offenses related to unauthorized software. At a very minimum, it would reasonably tend to reduce punishment. If it can be shown that every other soldier in PFC Manning's unit also downloaded software that was not on the approved list, this would certainly bear on the punishment that PFC Manning should receive for these particular offenses (which carry with them a maximum period of 4 years of confinement combined).

14. The Defense believes that if PFC Manning had only been charged with the offense of adding unauthorized software to a government computer, the Government would not be maintaining the position it is. The Government cannot fulfill its *Brady* obligations simply by turning over evidence that this favorable to the Defense in that it tends to reduce guilt or punishment of the *more serious* offenses. *Brady* applies equally to all offenses.

15. There is clear evidence that many soldiers added "unauthorized" software to computers. Now that the Government has this knowledge, it cannot simply ignore it. It has the independent obligation to search the computers to turn over evidence that falls within R.C.M. 701(a)(6). Moreover, the request for a list of software programs on the relevant computer is squarely within the parameters of R.C.M. 701(2)(A), which provides that all tangible items in the Government's possession, custody or control must be turned over if they are "material to the preparation of the Defense." As argued in the Motion to Dismiss, the standard of materiality is not a high one. *See, e.g., United States v. Roberts* 59 M.J. 323 (C.A.A.F. 2004)(" The defense had a right to this information because it was relevant to SA M's credibility and was therefore material to the preparation of the defense for purposes of the Government's obligation to disclose under R.C.M. 701(a)(2)(A).").

16. The Court ruled on 23 March 2010 that a complete search of the hard-drives was not material to the preparation of the defense for the charged specifications. However, the Court directed the Government to "search each of the 14 hard drives [for] Wget, M-IRC Chat, Google Earth, moves, games, music, and any other specifically requested program from the Defense." *See* Ruling: Defense Motion to Compel Discovery, p. 11. When the Defense consulted with its computer experts, it learned that this process was not likely to yield meaningful results in terms of getting access to the information sought – i.e. exactly how pervasive was the practice of adding unauthorized software in the SCIF? The Defense's expert proposed an alternative means of searching the relevant computers which would be minimally cumbersome for the Government and would yield the results sought by the Defense.

17. The Government has resisted this proposed approach, indicating instead that the Defense must submit a list of software programs that the Government will then specifically search for.

Moreover, it allows the Government to undercut the Defense's theory by calling rebuttal witnesses – all while having access the ***actual forensic*** results and not disclosing them to the Defense. In short, the Government should not be able to remain willfully blind and then call rebuttal witnesses to suggest that the practice was not widespread when it has evidence in its possession that could verify the facts either way. Further, unit witnesses are not likely to be forthcoming with whether they did, in fact, add unauthorized software to computers as this would incriminate them and subject them to criminal prosecution for violating a lawful general regulation.

Unfortunately, this misses the point of the entire discovery request. The point was to see how many other unauthorized software programs were found on the computers in the SCIF. If the Defense submits a list with, say, 50 different software programs and 5 of them are found on the relevant hard drives, this does not prove anything. It simply proves that these 5 random software programs were on some or all of the hard drives. It does not speak to the pervasiveness of the practice of adding authorized programs to government computers.

18. The Defense's computer experts have indicated that there are over 5 billion records of software in the Global Software Registry. To prepare a list that the Government will then look for is like playing a game of "Battleship" where the Defense has to guess which particular programs a soldier in PFC Manning's SCIF might have downloaded.[3] If the Defense guesses correctly, then that might be some proof (however limited) that others downloaded unauthorized software. If the Defense guesses incorrectly, which it is apt to do given the number of software programs out there, this does not prove anything. It simply shows—to use the Battleship analogy—that the Defense has not guessed the right coordinates.

19. The Government further resists performing the search requested by the Defense on the grounds that it is likely to yield classified data.[4] The Defense has trouble understanding how a screen shot of program/software names will yield classified data. But, to the extent that it does, the Defense has requested that the Government simply redact the classified information and state something to the effect of, "Program X, not on approved software list." The Defense is not interested in the *names* of the programs, or even the *types* of programs—simply the *number* of programs that appear on the hard drives that are not on the approved software list. Additionally, under the process recommended by Mr. Struttmann, the concern of the Government is eliminated (based upon the Government's representation during the 802 conference that it was unaware of any classified programs on the DCGS-A computer).

20. The Defense has proposed a simple, common-sense way of proceeding that avoids the potential disclosure of classified information. And yet, the Government inexplicably opposes the request. If the results of the proposed search are favorable, then they are *Brady* material which the Government must disclose. If the results of the search are unfavorable (i.e. no other soldier added software to his/her computer), then that evidence will be helpful to the Government's

[3] Battleship is a guessing game involving two players. The game is played on four grids, two for each player. The grids are typically square – usually 10×10 – and the individual squares in the grid are identified by letter and number. On one grid the player arranges ships and records the shots by the opponent. On the other grid the player records his/her own shots. Before play begins, each player arranges a number of ships secretly on the grid for that player. Each ship occupies a number of consecutive squares on the grid, arranged either horizontally or vertically. The number of squares for each ship is determined by the type of the ship. The ships cannot overlap (i.e., only one ship can occupy any given square in the grid). After the ships have been positioned, the game proceeds in a series of rounds. In each round, each player's turn consists of announcing a target square in the opponent's grid which is to be shot at. If a ship occupies the square, then it takes a hit. The player's opponent announces whether or not the shot has hit one of the opponent's ships and then takes a turn. When all of the squares of a ship have been hit, the ship is sunk. After all of one player's ships have been sunk, the game ends and the other player wins. *See* http://en.wikipedia.org/wiki/Battleship_(game).

[4] The fact that unauthorized program names may hypothetically yield classified information is not a reason to refuse to conduct a *Brady* search or to turn over specifically-requested items pursuant to R.C.M. 701(a)(2). As stated in the Court's order, "*Brady*, RCM 701(a)(2), 701(a)(6), and 701(g) govern discovery of both classified and unclassified information." (Ruling: Defense Motion to Compel Discovery, pg. 10).

prosecution of this offense.[5] Given this, it is difficult to understand the Government's opposition to the Defense proposal.

CONCLUSION

21. In light of the foregoing, the Defense requests that this Court order the Government to review the hard drives of the 14 computers using either of the methods proposed by the Defense's experts.

Respectfully submitted,

DAVID EDWARD COOMBS
Civilian Defense Counsel

[5] Such information would also be helpful to the Defense within the meaning of R.C.M. 701(a)(2) in that it may signal to the Defense that, as a trial strategy, this avenue is not worth pursuing.